



Employee Name

Department

## TOWN OF AMHERST TECHNOLOGY ACCEPTABLE USE POLICY

Updated: 05/09/2012

### Purpose:

The purpose of this policy is to prevent misuse of the Town's technology systems, to protect the Town from liability that could result from such misuse and to promote appropriate use and communication among staff and between staff and citizens.

All Town employees, board members, committee members, interns and contractors with user level access Town technology systems are required to read and comply with this policy. Failure to comply with this policy may result in disciplinary action up to and including termination of employment.

This policy applies to the use of all technology systems. Technology systems include all electronic hardware, software; landline phones, cell phones, smartphones, voicemail, tablet computers, desktop computers, laptop computers, fax/copy machines, printers, peripherals, door access and alarm systems, camera systems, software programs and databases, local and wide area networks, email and collaboration systems, internet.

This policy will be periodically reviewed and may be updated or amended at any time at the discretion of the Town Manager.

### Prohibitions:

The following activities are strictly prohibited because they violate the law:

Any illegal activity, including, but not limited to the transmission of copyrighted, trademarked, patented, trade secret material or the participation in any type of criminal activity;

Any illegal activity, including but not limited to the transmission or inquiry of obscene, defamatory, discriminatory, or threatening material;

Any attempts to tamper with or violate the computer security systems implemented by the Town or other institutions, organizations, companies or individuals.

The following activities are strictly prohibited because they violate Town policies, are inappropriate uses of Town owned equipment and facilities or may be objectionable and/or disrespectful to fellow employees and to citizens:

Technology systems shall not be used for personal, family, volunteer, civic, social or religious purposes, except for work-related professional or civic purposes. Technology systems may be used, with permission of an employee's supervisor, for brief family or personal business messages when such messages cannot be scheduled for breaks, lunch or before or after work. Except in emergencies, personal long-distance telephone calls shall not be charged to the Town.

Initials

Computers with access to the Internet, but not to the internal network, will be available at various locations for employees to use for such purposes during lunch or breaks.

Departments heads are responsible for determining which staff require regular use of a cell phone or combination cell phone/PDA with data plan, to efficiently and safely perform their primary function. Department heads will submit a detailed purchase order for Town Manager approval annually, and anytime a staff person is to be added to the reimbursement plan. Except in emergencies, use of any Town owned and provided cell phone for personal use is prohibited. Staff requiring regular use of a cell phone are eligible for a quarterly (every three months) reimbursement of one hundred and five (105) dollars if a personal cell phone account is established and maintained for Town business use. Staff requiring regular use of a cell phone/PDA with data plan are eligible for a quarterly (every three months) reimbursement of two hundred and ten (210) dollars if a personal cell phone account with a data plan is established and maintained for Town business use. Periodically without notice the Town will require proof that a staff person is maintaining and utilizing an operational cell phone for Town business use. Under certain circumstances a department head may request a larger onetime or ongoing cell phone reimbursement with the approval of the Town Manager.

Technology systems shall not be used for personal, for-profit activities, such as consulting for pay or for work performed for another employer.

Technology systems shall not be used to solicit contributions for personal activities, for outside organizations or other non-work related purposes, no matter how good the cause.

Users shall not view or disseminate images or content containing crude language, nudity, sexual activity or violence, unless required to do so by their job.

Users who synchronize or store Town information on a portable device such as a smartphone, tablet, netbook or laptop, owned personally or by the Town, shall set the device to require a passcode prior to each use. In the event such a device is lost or stolen, users shall report the device lost or stolen to the IT Department immediately. Users acknowledge by setting up synchronization with Town information, such as Exchange which includes email, contacts, calendars and reminders, this gives the IT Department the ability to remote wipe such a device if the device is lost or stolen.

Sensitive Town information, such as personnel information, shall not be exported, emailed, or downloaded to a storage device such as a thumb drive, without written email approval from a Department Head.

All technology acquisitions and implementations to be supported or maintained by the IT Department or requiring interaction with technology systems supported or maintained by the Information Technology Department, require approval of the Information Technology Director. The acquisition or installation of licensed software is strictly prohibited unless approved by the Information Technology Director.

Users shall not use another user's network account or password to access computers or technology systems. If access is needed to another user's files or applications, the IT Department will provide an alternate method for the access with written or verbal authorization from that user's department head.

Users shall not give their username or password to other Town staff or non-Town staff, including family members, for use at any time. Users are responsible for reporting any known non-Town staff use of Town technology systems to the IT Department immediately.

Technology systems shall not be used to distribute chain letters, to participate in “chat rooms” or bulletin boards (unless they are work-related) or to play computer games.

Technology systems shall not be used to proselytize or advertise for religious or political causes.

Email, the internal network, and the Internet should not be used for communications that express anger or criticism or which deliver “bad news,” such as the denial of an employee request. Such communications, when they are necessary, should be in person, whenever possible, or by telephone or in carefully worded written form when face-to-face communication is impossible or inappropriate.

## **Responsibilities and Expectations:**

Access to the Internet at work is for work-related purposes, it is neither a right nor a perk. Therefore, employees who are provided such access shall be responsible for appropriate use in accordance with this Technology Policy.

Emails, internet usage logs, files and documents other than those specifically exempt by state law are public records and may be obtained by the public (including the press) regardless of the reason or motive for the request. Employees should not expect that email messages and any other files, even those marked “personal”, are private or confidential.

Users are reminded all laws related to open, public meetings apply to the use of all technology systems.

Users are expected to undertake precautions to prevent infection of Town computers by computer viruses. In particular, software shall not be downloaded or installed from the internet unless they have been authorized by and subjected to virus detection procedures approved by the Information Technology Department. The Information Technology Director may, from time to time, impose additional restrictions or regulations on the installing of files and programs and such restrictions or regulations shall be considered part of this policy.

For external message correspondence, staff is expected to apply the same grammatical quality and professional letter writing standards that are applicable to paper-based correspondence, depending upon the staff person's relationship to the external email recipient. Email correspondence should reflect the Town's commitment to quality, performance and professionalism at all levels.

For internal message correspondence staff is expected to exercise good judgment regarding form and content. Language and content that are inappropriate in traditional forms of communication are not appropriate in electronic communications.

Users are expected to be energy conscious. Computers shall be powered off anytime they will not be used for two or more consecutive hours. Copiers and printers shall be powered off anytime they will not be used for twenty-four or more consecutive hours. Necessary exceptions are permitted with a Department Head's approval.

All laws and Town policies related to sexual harassment apply to the use of Town technology systems.

The Information Technology Department is responsible for periodic audit, without prior notice, of equipment and systems to ensure that violations of this policy do not occur.

The Information Technology Department may periodically take control of a user's computer remotely to troubleshoot problems and apply software updates.

The Information Technology Department is responsible for appropriate security measures, including the maintenance of password systems and configuring computers to lock after a period of inactivity. Employees are responsible for complying with these security measures by following procedures established for secure and private use of passwords and other procedures that may be established to enhance security of Town systems.

Department Heads and supervisors are responsible for requesting additions, changes, and deletions from network access for all of their employees by completing and submitting a Technology Resource Access Form. Department Heads and supervisors are also responsible for ensuring that all of their employees using the Town's technology systems have read this policy and understand its applicability to departmental activities.

### **Compliance:**

The Information Technology Department monitors and logs all activities on the town-wide system. Upon the request of the Town Manager or of a Department Head with the approval of the Town Manager, monitoring of technology systems usage by an employee, without notice may occur.

Reasons for monitoring may include, but are not limited to review of employee productivity or inappropriate behavior, investigations into claims of possible criminal activity and investigations into violations of this policy.

In addition to reviewing logs, emails and files of a suspected violator, monitoring techniques may include the installation and use of software designed to capture and archive the keystrokes and screen activity of a computer. The deletion by users of emails, documents and internet site histories do not delete those items from permanent electronic archives that are subject to monitoring.

Any person with questions regarding the application or meaning of this policy should seek clarification from appropriate management.

### **Violations:**

Department Heads and the Town Manager will review alleged violations of this policy on a case-by-case basis. Violations of this policy may result in appropriate disciplinary action under Town Personnel Procedures or Union Contracts, up to and including termination of employment and referral to appropriate law enforcement authorities.

---

**By signing below I acknowledge I have read and understood this policy:**

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date